FIG. 1

[登録フェーズ]

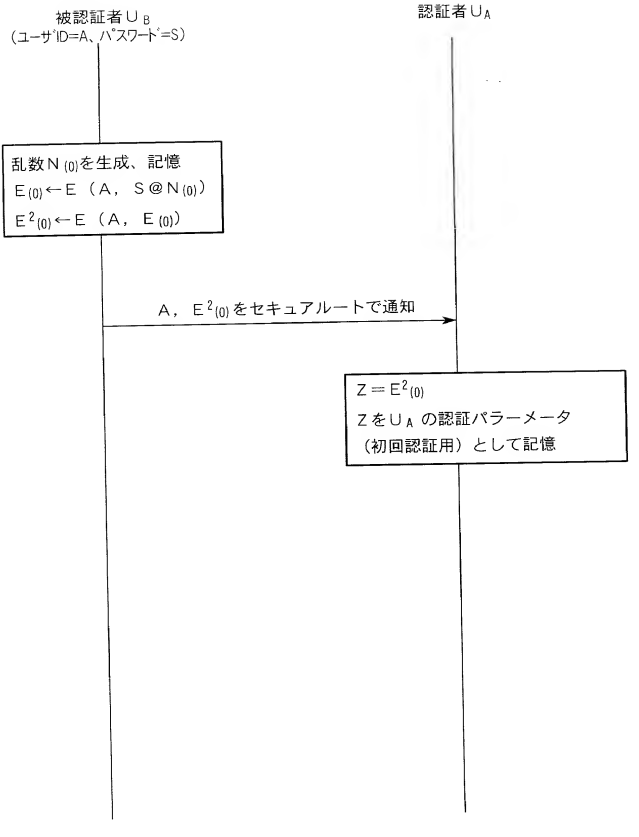

被認証者 U_B
（ユーザID=A、パスワード=S）
認証者 U_A
乱数 $N_{(0)}$ を生成、記憶
$E_{(0)} \leftarrow E$（A，$S \oplus N_{(0)}$）
$E^2_{(0)} \leftarrow E$（A，$E_{(0)}$）
A，$E^2_{(0)}$ をセキュアルートで通知
$Z = E^2_{(0)}$
Z を U_A の認証パラーメータ
（初回認証用）として記憶

FIG. 2

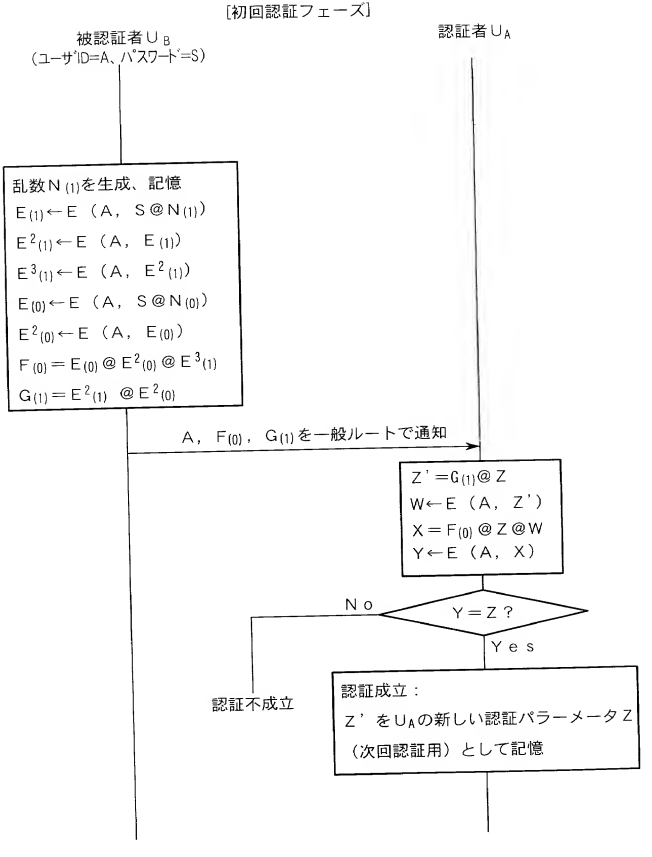

[初回認証フェーズ]
被認証者 U_B
(ユーザID=A、パスワード=S)
認証者 U_A
乱数 $N_{(1)}$ を生成、記憶
$E_{(1)} \leftarrow E$ (A, S@$N_{(1)}$)
$E^2_{(1)} \leftarrow E$ (A, $E_{(1)}$)
$E^3_{(1)} \leftarrow E$ (A, $E^2_{(1)}$)
$E_{(0)} \leftarrow E$ (A, S@$N_{(0)}$)
$E^2_{(0)} \leftarrow E$ (A, $E_{(0)}$)
$F_{(0)} = E_{(0)} @ E^2_{(0)} @ E^3_{(1)}$
$G_{(1)} = E^2_{(1)} @ E^2_{(0)}$
A, $F_{(0)}$, $G_{(1)}$ を一般ルートで通知
$Z' = G_{(1)} @ Z$
$W \leftarrow E$ (A, Z')
$X = F_{(0)} @ Z @ W$
$Y \leftarrow E$ (A, X)
No
Y = Z ?
Yes
認証不成立
認証成立：
Z' を U_A の新しい認証パラーメータ Z
(次回認証用) として記憶

FIG. 3

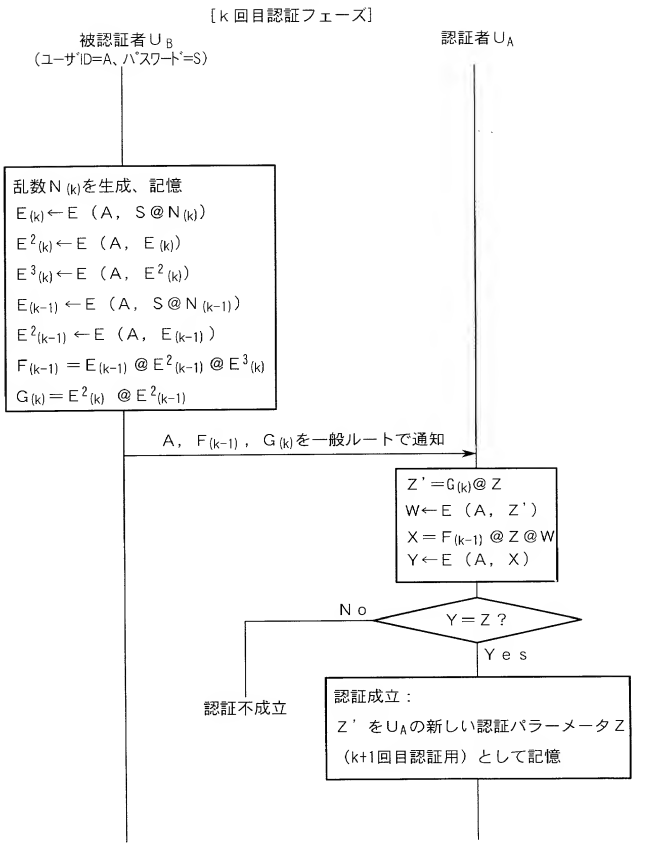
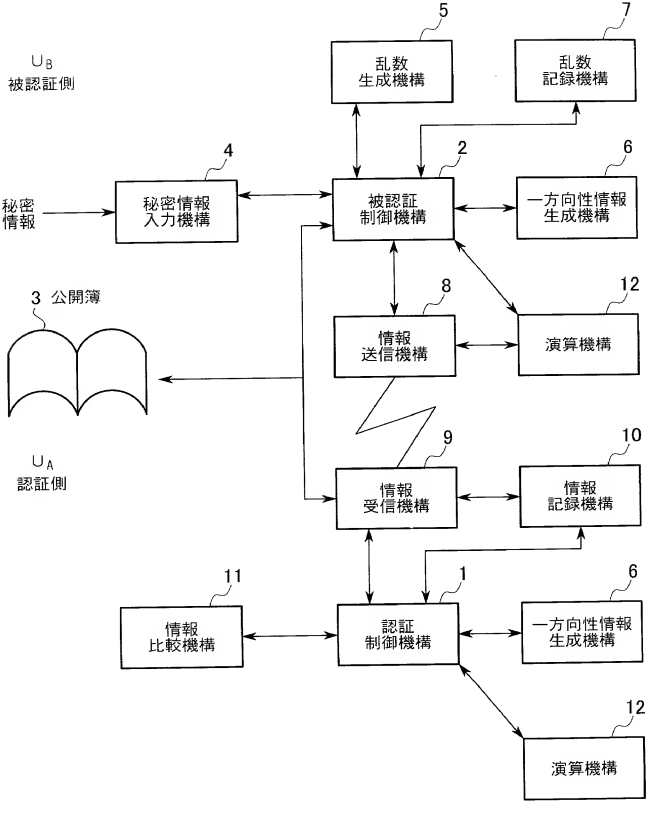

[k 回目認証フェーズ]
被認証者 U_B
(ユーザID=A、パスワード=S)
認証者 U_A
乱数 $N_{(k)}$ を生成、記憶
$E_{(k)} \leftarrow E\ (A,\ S @ N_{(k)})$
$E^2_{(k)} \leftarrow E\ (A,\ E_{(k)})$
$E^3_{(k)} \leftarrow E\ (A,\ E^2_{(k)})$
$E_{(k-1)} \leftarrow E\ (A,\ S @ N_{(k-1)})$
$E^2_{(k-1)} \leftarrow E\ (A,\ E_{(k-1)})$
$F_{(k-1)} = E_{(k-1)} @ E^2_{(k-1)} @ E^3_{(k)}$
$G_{(k)} = E^2_{(k)} @ E^2_{(k-1)}$
A, $F_{(k-1)}$, $G_{(k)}$ を一般ルートで通知
$Z' = G_{(k)} @ Z$
$W \leftarrow E\ (A,\ Z')$
$X = F_{(k-1)} @ Z @ W$
$Y \leftarrow E\ (A,\ X)$
No
$Y = Z$?
Yes
認証不成立
認証成立：
Z' を U_A の新しい認証パラーメータ Z
(k+1回目認証用) として記憶

FIG. 4


U_B
被認証側
5
乱数
生成機構
7
乱数
記録機構
4
秘密情報
入力機構
秘密
情報
2
被認証
制御機構
6
一方向性情報
生成機構
3 公開簿
8
情報
送信機構
12
演算機構
U_A
認証側
9
情報
受信機構
10
情報
記録機構
11
情報
比較機構
1
認証
制御機構
6
一方向性情報
生成機構
12
演算機構